(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

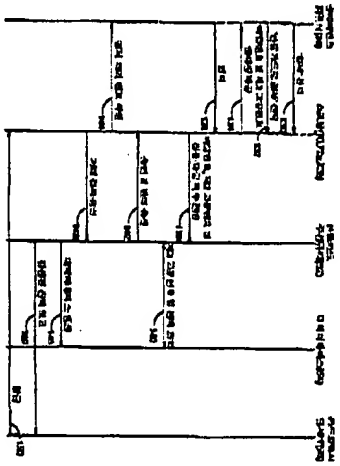
(11)Publication number: 000049518 A
(43)Date of publication of application: 05.08.2000

(21)Application number: 000017381
(22)Date of filing: 03.04.2000
(51)Int. Cl G06F 17/60

(71)Applicant: GIFT PD CORPORATION
(72)Inventor: AHN, JAE SIN

(54) METHOD FOR ISSUING PREPAYMENT CARD, AND METHOD FOR AUTHENTICATING PREPAYMENT CARD AND MANAGING BALANCE DATA

(57) Abstract:



PURPOSE: A method for issuing a prepayment card, authenticating the prepayment card and managing balance data, is provided to manage a utilization history in real time, by managing two random numbers by the account and balancing an account in every electronic commerce and face-to-face deal. Also, the method enables a card possessor to input a second specific number printed in a card of the card possessor himself/herself through Internet or an automatic response system(ARS), and to inquire every deal history including electronic commerce and a face-to-face deal.

CONSTITUTION: A method for issuing a prepayment card, which can be used in a charge payment based on authentication and balance management by a payment broker system in a face-to-face deal and electronic commerce, comprises the steps of: arranging card media; generating a first random number for authentication in a face-to-face deal, a second random number for authentication in electronic commerce; and recording information on the first random number, and the second random number in the card media.

Legal Status
Date of request for an examination (20000403)
Final disposal of an application (registration)
Date of final disposal of an application (20020227)
Patent registration number (1003300930000)
Date of registration (20020313)

【공개특허 제2000-49518호(2000.08.05) 1부.】

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7] G06F 17/60		(11) 공개번호	특2000-0049518
		(43) 공개일자	2000년08월05일
(21) 출원번호	10-2000-0017381		
(22) 출원일자	2000년04월03일		
(71) 출원인	기프트피디 주식회사 김석범		
(72) 발명자	서울특별시 영등포구 여의도동 14-31 한양빌딩 안지신		
(74) 대리인	서울특별시 강남구 압구정동 466번지 현대아파트 81동 207호 권용남		

심사청구 : 있음

(54) 선불카드 발행 방법과 선불카드 인증 및 잔액 데이터 관리방법

요약

대면거래에서는 물론 전자상거래에서도 사용할 수 있는 선불카드를 발행하는 방법과, 이와 같이 발행된 선불카드를 소지한 사람이 대면거래 또는 전자상거래를 행하고자 할 때 선불카드를 인증하고 잔액 데이터를 관리하는 방법을 제공한다.

선불카드를 발행함에 있어서는, 먼저, (a) 카드 매체를 마련한 후, (b) 대면거래 시의 인증을 위한 제1 난수와, 전자상거래 시의 인증을 위한 제2 난수를 발생한다. 그 다음, (c) 상기 제1 난수에 관한 정보 및 제2 난수를 상기 카드 매체에 기록하게 된다. 카드 매체는 정보 저장 수단을 포함하고 있는 것이 바람직하다. 이러한 경우 제1 난수 정보는 상기 정보 저장 수단에 저장될 수 있다. 바람직한 실시예에 있어서, 제1 난수 정보는 제1 난수와 동일하며, 따라서 (c)단계에서는 제1 난수 그 자체를 저장한다. 그렇지만, 본 발명의 다른 실시예에 있어서는, 저장 전에 제1 난수를 암호화함으로써, 암호화된 제1 난수를 제1 난수 정보로써 저장할 수도 있다. 한편, 제2 난수를 카드 매체의 표면에 인쇄하는 방식으로 기록된다. 이때, 제2 난수가 인쇄된 카드 매체 표면 부분에 제2 난수가 노출되는 것을 방지하기 위해 피막을 입히는 것이 바람직하다.

대표도

도3

색인어

선불카드, 상품권, 인증, 승인, 난수, 잔액

명세서

도면의 간단한 설명

도 1은 본 발명에 의한 바람직한 실시예에 있어서 소비자에게 제공되는 상태를 보여주는 선불카드 표면도.

도 2는 사용자가 표면의 피막을 제거한 상태를 보여주는 선불카드 표면도.

도 3은 도 1의 선불카드의 배면도.

도 4는 도 1 내지 도 3에 도시된 선불카드 발행 과정을 보여주는 흐름도.

도 5는 본 발명에 의한 선불카드에 있어서 자기 스트립에 기록되는 데이터 포맷의 일 예를 보여주는 도면.

도 6은 본 발명의 방법을 구현하기 위한 선불카드의 인증 및 잔액 관리 시스템의 일 실시예의 구성도.

도 7은 카드 승인 단말기(CAT)의 일 예를 보여주는 도면.

도 8은 대면거래에 있어서의 선불카드 인증 절차를 보여주는 도면.

도 9는 전자상거래에 있어서의 선불카드 인증 절차의 일 실시예를 보여주는 도면.

도 10a 및 도 10b는 전자상거래에 있어서의 선불카드 인증 절차의 다른 실시예를 보여주는 도면.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 상거래를 위한 결제 수단에 관한 것으로서, 보다 상세하게는 상거래를 행하기 이전에 경제적 가치를 지불하고 구입하는 선불카드에 관한 것이다.

선불카드는 일종의 상품권으로서, 일정한 발행 금액이 기록된 상태로 고객에게 선매된 후 고객이 상기 발행 금액 내에서 자유롭게 사용하도록 하는 카드를 말한다. 이와 같은 선불카드는 통상 플라스틱이나 PET(Polyethylene Terephthalate) 재질로 되어 있으며, 일반적으로 신용카드와 같이 약 85 밀리미터(㎜)의 길이에 54 ㎜의 폭을 가지는 직방형으로서 모서리가 라운딩되어 있는 형태를 가지도록 제작된다. 카드의 이면에는 길이방향으로 어느 한 변과 평행하게 자기 스트립이 도포되어 있는데, 상품권으로써 자유롭게 운용될 수 있도록 하기 위해 상기 자기 스트립에는 카드의 고유번호 및 잔액이 암호화되어 기록된다. 이와 같은 종래의 선불카드는 통상 백화점이나 통신 서비스 업체 또는 다점포형 직영 체인점 등에 의해 개별적으로 발행되어 유통된다.

이와 같은 선불카드는 통상적으로 신용카드나 직불카드 결제를 위한 단말기와는 별도의 전용 단말기가 설치되어 있는 곳에서만 사용이 가능하다. 이에 따라, 선불카드를 취급하는 점포는 단말기 구입의 경제적 부담을 안게 된다. 구매자 입장에서도, 카드사용이 가능한 곳이 전용 단말기가 설치되어 있는 곳, 예컨대 해당 선불카드 발행 업체나 그 대리점 또는 이와 제휴한 점포로 제한되어 있음으로 말미암아, 자신이 선매하거나 또는 타인에게서 선물받은 선불카드를 유용하게 사용하기가 어렵다.

한편, 자기 스트립에 저장된 정보는 쉽게 독출될 수 있고 재기록될 수 있어서 기록된 정보의 위조 또는 변조가 용이하기 때문에, 종래의 선불카드는 보안성이 크게 결여되어 있다는 문제점이 있다. 이러한 단점을 해결하기 위하여, 일부 선불카드 특히 신용카드사 또는 신용카드 VAN 업체에서 발행하는 선불카드의 경우에는, 카드의 고유번호 등을 자기 스트립에 기록하는 대신에, 카드 구매 시에 구매자에게 고유번호 또는 비밀번호를 별도로 알려주는 방법을 채택하고 있다. 그렇지만, 이러한 카드는 사용 시에 사용자가 카드번호 또는 비밀번호를 키패드를 사용하여 입력하여야만 하는 불편함이 발생한다. 위조 및 변조 가능성을 줄이기 위해 선불카드를 IC카드 형태로 제작하거나 선불카드에 신용카드처럼 홀로그램을 새기는 것도 생각해 볼 수 있지만, 이러한 경우 카드 제작 원가가 크게 증가하게 되기 때문에 두세 번 이내만 사용되는 경우가 많은 선불카드에 대해서는 적합하지가 않다.

이와 관련하여 본 출원인은 1999년 4월 28일 출원된 특허출원 10-1999-0015282호(발명의 명칭: 선불카드의 인증 및 잔액 데이터 관리 방법 및 이를 위한 시스템)를 통해서, 선불카드 가맹점들의 설비비 부담을 경감시킬 수 있고 카드의 위조나 변조에 따른 카드 소지자나 발행업체의 예측치 못한 손해를 감소시킬 수 있는 선불카드 인증 및 잔액 데이터 관리 방법을 제안한 바 있다. 상기 선행 특허출원에 따르면, 각 선불카드의 잔액 정보가 해당 선불카드에는 기록되지 않고 카드 발행 업체 또는 관리 업체의 호스트 컴퓨터의 데이터베이스에 저장되어 유지된다.

또한, 선불카드에는 그 표면에 양각되어 있는 일련 번호와는 별개로 난수발생기에 의해 발생된 난수 또는 이러한 난수가 암호화된 데이터가 기록된다. 이러한 난수 또는 암호화된 난수는 상기 호스트 컴퓨터의 데이터베이스에도 저장되어 있다. 상품 구매 시에, 호스트 컴퓨터는 선불카드에서 독출된 난수 또는 암호화된 난수를 데이터베이스에 저장된 것과 비교하여 카드를 인증하게 된다. 이처럼 난수를 사용하는 경우, 선불카드의 위조 또는 변조가 어려워지고 위조 및 변조에 따른 피해 정도가 줄게 된다. 또한 선불카드를 사용함에 있어서 기존의 신용카드 승인 단말기 또는 POS 단말기를 통해 인증을 받기 때문에 선불카드 가맹점들의 설비비 추가 부담이 거의 없어지며, 구매자의 입장에서 선불카드의 효용이 증대될 수 있다.

한편, 인터넷 이용자 수 증가와 더불어 전자상거래가 최근 급속히 성장하고 있다. 전자상거래에 의한 상품 구매에 따른 대금 지불에 있어서는 다양한 방법들이 사용되고 있는데, 이러한 방법들의 예로는 신용카드나 전자화폐를 사용하는 것 등을 들 수 있다. 그렇지만, 현재까지 실험적으로 사용되고 있거나 제시된 바 있는 전자상거래 지급결제 수단 중에, 대면거래에 사용되는 선불카드를 활용하는 방식은 아직 없다. 이는, 위에서 기술한 바와 같이 종래의 선불카드는 대부분이 잔액 정보를 자기 스트립에 저장하고 있어서 단말기가 없는 한 이 정보를 확인하기 어렵기 때문이다.

이와 관련하여, 전자화폐 중에서 지불 브로커 시스템의 인증을 받아 사용할 수 있는 네트워크형 전자캐쉬는 대면거래에 있어서 선불카드와 같은 기능을 수행한다. 이러한 전자캐쉬는 신용카드나 현금을 주고 구입할 수 있으며, 잔액이 거의 없는 경우 경제적 가치를 지불하고 다시 잔액을 충전할 수 있고 다른 사람에게 이전할 수도 있게 되어 있다. 그렇지만, 대면거래에 사용되는 선불카드를 전자상거래에 사용할 수 없는 것과 마찬가지로, 전자캐쉬는 전자상거래에서만 사용할 수 있을 뿐이고 대면거래에는 사용할 수 없다는 단점이 있다.

발명이 이루고자하는 기술적 과제

본 발명은 상술한 문제점을 해결하기 위한 것으로서, 대면거래에서는 물론 전자상거래에서도 사용할 수 있는 선불카드를 발행하는 방법을 제공하는 것을 그 기술적 과제로 한다.

아울러, 본 발명은 이와 같이 발행된 선불카드를 소지한 사람이 대면거래 또는 전자상거래를 행하고자 할 때 상기 선불카드를 인증하고 잔액 데이터를 관리하는 방법을 제공하는 것을 다른 기술적 과제로 한다.

발명의 구성 및 작용

상기 기술적 과제를 달성하기 위한 선불카드 발행 방법에 따르면, 먼저, (a) 카드 매체를 마련한 후, (b) 대면거래 시의 인증을 위한 제1 난수와, 전자상거래 시의 인증을 위한 제2 난수를 발생한다. 그 다음,

(c) 상기 제1 난수에 관한 정보 및 제2 난수를 상기 카드 매체에 기록하게 된다. 카드 매체는 정보 저장 수단을 포함하고 있는 것이 바람직하다. 이러한 경우 제1 난수 정보는 상기 정보 저장 수단에 저장될 수 있다. 바람직한 실시예에 있어서, 상기 제1 난수 정보는 상기 제1 난수와 동일하며, 따라서 (c)단계에서 쓰인 제1 난수 그 자체를 저장한다. 그렇지만, 본 발명의 다른 실시예에 있어서는, 저장 전에 제1 난수를 암호화함으로써, 암호화된 제1 난수를 제1 난수 정보로써 저장할 수도 있다. 한편, 제2 난수를 카드 매체의 표면에 인쇄하는 방식으로 기록된다. 이때, 제2 난수가 인쇄된 카드 매체 표면 부분에 제2 난수가 노출되는 것을 방지하기 위해 피막을 입히는 것이 바람직하다.

상기 다른 기술적 과제를 달성하기 위한 선불카드 인증 및 잔액 데이터 관리방법은 일종의 지불 브로커 시스템을 기반으로 하여 운영되며, 복수의 고유번호들이 기록된 선불카드에 의해 상품 결제 대금을 결제할 수 있도록 해준다. 여기서, 복수의 고유번호들은 난수 발생기에 의해 발생되는 제1 및 제2 난수를 토대로 각각 결정되는 제1 및 제2 고유번호를 포함한다.

인증 및 잔액 데이터 관리방법에 따르면, 먼저 (a) 카드 승인을 위한 단말기와, 상기 제1 및 제2 고유번호와 등록할 것이 요구되는 제1 및 제2 발행 고유번호와 잔액 데이터를 저장하는 호스트를 제공한다. 여기서, 상기 단말기는 신용카드 승인 단말기 또는 POS단말기 중에서 선택되는 것이 바람직하다. (b) 구매자가 대면거래를 통해 상기 상품을 구매하고자 하는 경우, 단말기를 통해 상기 제1 고유번호 및 제1 결제대금 데이터를 받아들이고 제1 고유번호 및 제1 결제대금 데이터를 각각 제1 발행 고유번호 및 잔액 데이터와 비교한다. (c) 상기 (b)단계에서 제1 고유번호 및 제1 발행 고유번호가 서로 동일하고 잔액이 0이 아닌 경우 승인액 만큼의 선불카드 사용을 승인한다. 이때, 잔액이 상기 제1 결제대금보다 많은 때에는 상기 승인액은 제1 결제대금이고 잔액이 제1 결제대금보다 적은 때에는 상기 승인액은 잔액과 동액이 된다.

(d) 구매자가 전자상거래를 통해 상기 상품을 구매하고자 하는 경우에는, 전자상거래가 이루어지는 머천트 서버로부터 제2 고유번호 및 제2 결제대금 데이터를 받아들이고 제2 고유번호 및 제2 결제대금 데이터를 각각 제2 발행 고유번호 및 잔액 데이터와 비교한다. (e) 상기 (d)단계에서 제2 고유번호 및 제2 발행 고유번호가 서로 동일하고 잔액이 0이 아닌 경우 승인액 만큼의 선불카드 사용을 승인한다. 이때, 잔액이 제2 결제대금보다 많은 때에는 상기 승인액은 제2 결제대금이고 상기 잔액이 상기 제2 결제대금보다 적은 때에는 상기 승인액은 잔액과 동액이 된다. (f) 상기 (c) 또는 (e)단계에서 선불카드의 사용을 승인한 경우에는, 잔액에서 승인액을 차감하여 차감된 잔액을 수정된 잔액으로서 다시 저장하게 된다.

이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 보다 구체적으로 설명한다.

도 1 내지 도 3은 본 발명의 바람직한 실시예에 따른 선불카드의 형태를 보여준다. 선불카드(10)는 플라스틱이나 PET 재질로 되어 있으며, 약 85 밀리미터(mm)의 길이에 54 mm의 폭을 가지는 정방형으로서 모서리가 라운딩되어 있는 형태를 가진다. 카드의 표면에는 발행업체의 로고 및 금액을 포함한 디자인이 인쇄되어 있고, 카드의 배면에는 길이방향으로 상변과 평행하게 적어도 한 라인의 자기 스트립(18)이 도포되어 있다. 본 발명에 의한 선불카드의 발행업체로는 예컨대 백화점이나 정유사, 주유소, 도서상품권 발행업체 또는 그 밖의 상품 유통업체들이 될 수 있다.

바람직한 실시예에 있어서, 선불카드(10)에는 세 개의 번호 즉, 하나의 일련번호와 두 개의 고유번호가 기입된다. 도 1 및 도 2에 도시된 바와 같이, 일련번호(12)는 카드의 정면에 양각하는 방식으로 기입되며, 외부에 노출되어 있다. 첫 번째 고유번호는 카드발행업자의 난수 발생기에 의해 생성되며, 배면의 자기 스트립(18)에 기록된다. 특히 본 발명에 있어서 선불카드의 자기 스트립이 신용카드에 일반적으로 사용되는 것과 동일한 형태로 제작되는 경우, 상기 첫 번째 고유번호는 자기 스트립의 트랙1 내지 트랙3 중 신용카드에 대한 정보가 통상 저장되는 트랙2에 저장되는 것이 바람직하다. 이러한 첫 번째 고유번호는 카드 소지자가 대면거래에 의해 상품을 구매하고자 할 때 카드를 인증하는데 사용된다.

두 번째 고유번호(16)는 마찬가지로 카드발행업자의 난수 발생기에 의해 생성되며, 도 2에 도시된 바와 같이 카드의 정면에 인쇄된다. 두 번째 고유번호(16)가 인쇄된 상태에서 인쇄 부분 상에는 즉석식 복권 등에서 볼 수 있는 피막(14)이 입혀진다. 따라서, 사용자가 표면의 피막(14)을 제거하지 않는 한, 두 번째 고유번호(16)는 외부에서 파악할 수 없게 되어 있다. 이러한 두 번째 고유번호는 카드 소지자가 전자상거래에 의해 상품을 구매하고자 할 때 카드를 인증하는데 사용된다.

도 4는 도 1 내지 도 3에 도시된 선불카드 발행 과정을 보여준다. 먼저, 제20단계에서 카드 매체를 마련한 후, 난수발생기를 사용하여 제1 난수 및 제2 난수를 발생한다(제32단계). 여기서, 제1 난수는 대면거래 시의 카드 인증을 위한 것이고, 제2 난수는 전자상거래 시의 카드 인증을 위한 것이다. 제1 및 제2 난수의 발생이 완료되면, 제1 난수를 자기 스트립(18)에 저장하고 제2 난수를 카드 표면에 인쇄하게 된다(제34단계, 제36단계). 마지막으로, 제2 난수가 인쇄된 카드 매체 표면 부분에 상기 제2 난수가 노출되는 것을 방지하기 위한 피막(14)을 입히게 된다(제28단계).

이와 같이, 바람직한 실시예에 있어서는 제1 난수 및 제2 난수가 직접 자기 스트립(18) 및 카드 표면에 기록되며, 따라서 정보는 제1 난수 및 제2 난수가 위에서 언급한 제1 고유번호(12) 및 제2 고유번호(16)에 해당한다. 그렇지만, 본 실시예가 변형된 다른 실시예에 있어서는, 제1 난수를 암호화하여 자기 스트립(18)에 저장할 수도 있다. 이러한 경우에는 암호화된 제1 난수가 제1 고유번호(12)에 해당하게 된다.

본 발명의 또 다른 실시예에 있어서는, 카드 매체(10)에 자기 스트립이 구비되지 않고, 제1 고유번호(12) 역시 카드 매체(10)의 표면 또는 배면에 직접 표시될 수도 있다. 이러한 경우에 있어서는, 대면거래시에 노출된 제1 고유번호(12)를 타인의 시선으로부터 차단할 수 있도록 PIN 패드를 사용하는 것이 바람직하다. 아울러, 본 발명의 또 다른 실시예에 있어서는, 카드 매체(10)가 집적회로 칩 및 안테나를 구비하는 IC카드 내지 스마트카드 형태로 제작될 수도 있다. 이러한 경우, 제1 고유번호(12)는 집적회로 칩에 저장될 수 있다.

도 5는 자기 스트립에 기록되는 데이터 포맷의 일 실시예를 보여준다. 기록되는 데이터는 카드 발행업체 식별번호(ID), 카드 고유번호 및 체크 비트를 포함한다. 바람직한 실시예에 있어서, 카드 발행업체 식별번호(ID)는 8 바이트로 되어 있으며, 선불카드를 발행한 업체의 고유 코드를 나타낸다. 카드 고유번호는

10 바이트의 크기를 가지며, 카드 발행 시에 난수발생기 프로그램에 의해 생성되는 난수로 되어 있다. 따라서, 카드 표면에 표기된 일련 번호가 연이어진 카드들간에도 카드 고유번호는 완전히 상이하게 되며, 이에 따라 변조의 목적을 가지고 어느 한 카드의 고유번호를 판독했다 해도 그 카드와 일련 번호가 연이어진 카드의 고유번호를 예측하는 것은 거의 불가능하게 된다. 예를 들어 상기 10 바이트의 카드 고유번호에 있어서 각 바이트가 10진수 한자리를 표시하는 경우에, 어느 한 카드의 고유번호를 임의로 예측할 때의 적중률은 1/10,000,000,0000이 된다. 한편, 체크 비트는 2 바이트의 크기를 가지며 기록 데이터의 유효성을 검증하는데 사용된다. 그밖에도, 카드 발행 업체나 인증 데이터를 중계 전송하는 VAN 사업자의 선택에 따라 추가적인 데이터가 기록될 수 있다.

도 6은 본 발명의 방법을 구현하기 위한 선불카드의 인증 및 잔액 관리 시스템의 구성을 보여준다. 인증 및 잔액 관리를 위한 시스템은 카드 승인 단말기(30), 카드 VAN 시스템의 호스트(40), 선불카드 주컴퓨터 부시스템(50) 및 카드발행사 웹서버(70)를 포함한다.

카드 승인 단말기(30)로는 신용카드 가맹점들에 설치되어 있는 종래의 카드 승인 단말기(Credit Authorization Terminal: CAT)가 사용된다. 특히, 위에서 기술한 바와 같이 선불카드의 자기 스트립이 신용카드에 일반적으로 사용되는 것과 동일한 형태로 제작되고 카드 고유번호가 신용카드에 있어서와 같이 트랙2에 저장되는 경우에는, 카드 승인 단말기(30)에 있어서 선불카드를 위한 별도의 헤드가 필요없게 되며 운용 프로그램을 간단하게 변경하는 것만으로 족하게 된다.

도 7은 이러한 CAT(30)의 일 예를 보여준다. CAT(30)의 외관은 대략 직육면체 형상으로 되어 있으며, 그 일 측에는 카드를 스와이핑(Swiping)하여 카드의 자기 스트립에 기록된 데이터를 판독하기 위한 슬롯(32)이 형성되어 있다. CAT의 상부면 내측에는 가맹점 주가 서비스 종류나 상품 판매 대금 등을 입력할 수 있도록 키패드(34)가 설치되어 있다. 또한, CAT의 상부면 외측에는 다량의 머리 전표 양식이 적재되어 있으며, 카드 승인 결과에 따라 매출 전표(36)가 발행된다. 상품 거래와 관련하여 특정 선불카드에 대한 인증 요청을 하고자 하는 경우, 가맹점 주는 키패드(34) 상의 "선불카드" 키를 누른 후 카드를 슬롯(32)에 삽입하여 스와이핑하게 된다. 그리고, 키패드(34)의 숫자 키를 사용하여 판매 대금을 입력하고 키패드(34) 상의 "전송"버튼을 누르게 된다. 이때 제1 고유번호 및 상품 대금 데이터를 포함한 인증 요청 메시지가 공중통신망을 통해 카드 VAN 호스트(40)로 전송된다.

다시 도 6을 참조하면, 카드 VAN 호스트(40)는 카드 VAN 사업자의 장비로서, 신용카드 및 직불카드에 대한 승인 요청 및 이에 대한 응답 데이터를 중계한다. 특히, 본 발명의 바람직한 실시예에 있어서 선불카드의 인증 및 잔액 관리 시스템은 기존의 신용카드 승인 시스템의 하부 구조를 토대로 구축되기 때문에, 카드 VAN 호스트(40)는 복수의 신용카드사 호스트(100a, 100b)에 접속되어 있다. 또한, 카드 VAN 호스트(40)는 전용회선을 통해 또는 회선 교환망을 통해 선불카드 주컴퓨터 부시스템(50)에도 접속되어 있으며, 이에 따라 CAT(30) 및 선불카드 주컴퓨터 부시스템(50)사이에서 본 발명에 의한 선불카드에 대한 승인 요청 및 이에 대한 응답 데이터를 중계할 수 있다.

선불카드 주컴퓨터 부시스템(50)은 주컴퓨터(52), 데이터베이스(54) 및 자동응답(ARS) 부시스템(56)을 포함한다. 데이터베이스(54)는 선불카드 주컴퓨터 부시스템(50) 운영자와 계약이 체결되어 있는 다수의 선불카드 발행업체들 각각에 의해 발행되는 모든 선불카드에 대한 일련 번호, 제1 및 제2 고유번호, 액면가, 잔액 및 거래 내역에 대한 데이터를 저장한다. 아울러, 데이터베이스(54)는 후술하는 바와 같이 각 선불카드의 소지자가 인터넷을 통해 등록하는 비밀번호를 추가적으로 저장할 수도 있다. 한편, ARS 부시스템(56)은 주컴퓨터(52)에 접속되어 있으며, 전화기(82)를 통해 선불카드 소지자가 자신의 카드 잔액을 조회할 수 있도록 해준다. 또한, ARS 부시스템(56)은 카드의 정당한 소지자가 카드를 도난당하거나 분실했을 때 타인의 사용을 제한해 줄 것을 요청하는 경우 이러한 요청을 처리한다.

CAT(30)로부터 카드 VAN 호스트(40)를 통해 선불카드 인증 요청이 있는 경우, 주컴퓨터(52)는 인증 요청 메시지에 포함된 제1 고유번호 및 상품 대금 데이터를 데이터베이스(54)에 저장된 고유번호 및 잔액과 각각 비교한 후, 카드 VAN 호스트(40)를 경유하여 CAT(30)에 인증 응답 메시지를 전송한다. 그리고, 인증 요청 메시지에 포함된 제1 고유번호가 데이터베이스(54)에 저장된 것과 동일하고 해당 카드의 잔액이 인증 요청 메시지에 포함된 판매 대금 액수보다 많아서 해당 카드의 사용을 승인한 경우, 주컴퓨터(52)는 데이터베이스(54)에 저장된 해당 카드 잔액에서 판매 대금 액수를 차감하고 차감된 금액을 수정된 잔액으로서 다시 데이터베이스(54)에 저장한다. 이때, 거래내역이 함께 저장될 수도 있다.

카드발행사 웹서버(70)는 각 카드 발행업체별로 마련된다. 카드발행사 웹서버(70)에 접속된 단말기(미도시됨)를 통해서 해당 업체의 담당자는 발행되는 선불카드들의 일련번호, 제1 및 제2 고유번호와, 초기 잔액을 선불카드 부시스템(50)에 전송할 수 있다. 또한, 카드 발행업체의 담당자는 선불카드 주컴퓨터 부시스템(50)으로부터 해당 업체에서 판매한 카드들 각각의 잔액 및 총잔액을 확인할 수도 있다. 한편, 본 발명의 다른 실시예에 있어서는, 선불카드 주컴퓨터 부시스템(50)이 주기적으로 또는 비주기적으로 각 카드발행사 웹서버(70)에 대하여 해당 업체에서 발행한 카드들 각각에 대한 잔액 데이터를 보고할 수도 있다. 이러한 선불카드 주컴퓨터 부시스템(50)과 카드발행사 웹서버(70)간의 상호작용을 위해, 주컴퓨터 부시스템(50)은 각 카드발행사에 대해 사용자 번호와 비밀번호를 사전에 부여할 수 있다.

카드 소지자는 자신의 클라이언트 컴퓨터(84)에 적재된 웹 브라우저를 사용하여 인터넷을 통해 웹서버(70)에 접속할 수 있다. 카드발행사 웹서버(70)는 접속된 클라이언트 컴퓨터(84)의 html 요구에 따른 html 응답으로써 전자상거래를 위한 비밀번호를 입력할 수 있는 입력창을 제공할 수 있다. 카드 소지자가 자신의 카드의 일련번호 및/또는 그 밖의 정보와 함께 비밀번호를 입력하면, 카드발행사 웹서버(70)는 수신된 비밀번호를 선불카드 주컴퓨터 부시스템(50)에 전송하여, 비밀번호가 데이터베이스(54)에 저장될 수 있도록 해준다.

본 발명에 의한 선불카드 발행업체들 중 적어도 일부는 사이버 쇼핑몰을 운영하는 회사들일 수 있다. 이러한 회사들의 카드발행사 웹서버는 카드 발행 및 관리 업무와 함께 쇼핑몰 서버로서의 기능을 병행하여 수행한다. 물론, 웹서버의 업무 부하와 컴퓨팅 능력을 고려하여, 카드 발행 및 관리 업무를 위한 호스트 컴퓨터와 쇼핑몰 운영을 위한 쇼핑몰 서버에 대해 물리적으로 별개의 컴퓨터를 사용할 수도 있다.

이와 같이 쇼핑몰 운영을 병행하는 카드 발행업체들의 웹서버(70)에서 상품을 구매하는 경우, 카드 소지

자는 자신이 주문한 상품(들)에 대해 선불카드로써 결제를 할 수가 있다. 이를 위해 웹서버(70)는, 결제를 위한 html 문서 또는 asp 문서 내에서, 선택가능한 결제 방법들 중 하나로 '선불카드로 결제' 버튼을 제시하게 된다. 만약, 카드 소지자가 선불카드에 의한 결제를 희망하는 경우, 카드발행사 웹서버(70)는 카드 소지자에 대해 비밀번호 및 제2 고유번호를 입력하도록 한 후, 비밀번호 및 제2 고유번호와 결제 금액을 선불카드 주컴퓨터 부시스템(50)에 전송하여 인증을 받게 된다. 전자상거래를 위한 인증 과정은 카드 VAN 호스트(40)를 통한 대면거래의 인증 과정과 유사하다.

한편, 본 발명에 의한 선불카드는 카드발행사 웹서버(70) 이외의 쇼핑몰들(72a, 72b)에서 상품을 구매하는 경우에도 활용될 수 있다. 이와 같이 선불카드에 의한 결제가 허용되는 쇼핑몰들은 각 카드 발행업체 또는 선불카드 주컴퓨터 부시스템(50) 운영자와 해당 쇼핑몰 운영자간의 계약에 의해 정해질 수 있다. 쇼핑몰(72a 또는 72b)에서의 주문, 결제 및 카드 인증 과정은 카드발행사 웹서버(70)가 운영하는 쇼핑몰에서의 과정과 유사하므로 이에 대한 자세한 설명은 생략한다.

본 발명의 일 실시예에 있어서는, 위에서 기술한 바와 같이 쇼핑몰(70, 72a, 72b)에서 직접 비밀번호 및 제2 고유번호를 받아들이고, 이를 선불카드 주컴퓨터 부시스템(50)에 전송하여 인증을 받는다. 그렇지만, 본 발명의 다른 실시예에 있어서는, 결제를 위한 웹 페이지에서 '선불카드로 결제' 버튼을 누른 후 '확인' 버튼을 누르게 되면 웹 브라우저가 상기 '확인' 버튼에 하이퍼링크되어 있는 선불카드 주컴퓨터 부시스템(50)에 접속된다. 이때, 하이퍼링크된 선불카드 주컴퓨터 부시스템(50)의 웹 페이지 URL에는 결제 금액에 관한 정보가 헤더로써 포함된다.

카드 소지자는 선불카드 주컴퓨터 부시스템(50)이 제공하는 인증 웹 페이지 상의 입력창에 비밀번호 및 제2 고유번호를 입력할 수 있다. 주컴퓨터(52)는 제2 고유번호, 비밀번호 및 상품 대금 데이터를 데이터베이스(54)에 저장된 데이터들과 각각 비교한다. 비교 결과에 따라, 인증 확인 asp 파일이 클라이언트 컴퓨터(84)로 전송된다. 인증 확인 asp 파일에는 인증 결과를 알리는 메시지와 함께 '쇼핑몰로 되돌아가기' 버튼이 포함되어 있다. 카드 소지자가 '쇼핑몰로 되돌아가기' 버튼을 누르면, 다시 쇼핑몰 웹서버(70, 72a, 72b)에 접속이 되어 결제가 처리된 후 상거래 세션이 종료된다. 상거래 세션이 종료되면, 쇼핑몰 웹서버(70, 72a, 72b)는 결제 완료 메시지를 주컴퓨터(52)에 전송하여, 데이터베이스(54)에 저장된 잔액 데이터가 갱신될 수 있게 해준다. 한편, 쇼핑몰로의 복귀를 원활하게 하기 위해 쿠키(Cookies)가 활용될 수도 있다.

전자상거래를 위한 쇼핑몰의 구성 및 운영, 하이퍼링크에 의한 페이지 이동, 쿠키(Cookies)의 활용 등은 본 발명이 속하는 기술 분야 특히 인터넷 비즈니스 분야에서 보통 정도의 지식을 가진 자가 용이하게 구현할 수가 있다. 그러므로 이들에 대한 구체적인 설명은 생략한다.

도 8 내지 도 10을 참조하여, 대면거래 및 전자상거래에 있어서의 선불카드 인증 절차를 보다 구체적으로 설명한다.

도 8은 대면거래에 있어서의 선불카드 인증 절차를 보여준다. 구매자가 상품 대금을 선불카드로 결제하기를 희망하는 경우, 가맹점주는 CAT(30)에 의해 선불카드(10)의 자기 스트립(18)에 저장된 데이터를 독출하고 판매 대금 액수를 입력한 후 '전송'키를 누르게 된다(제100단계). 이에 따라, 카드 발행 업체 10, 카드의 제1 고유번호 및 사용 금액을 포함한 인증 요청 메시지가 VAN 호스트(40)로 전송된다(제102단계). VAN 호스트(40)는 해당 메시지가 선불카드에 대한 것임을 인식하고 메시지의 내용을 선불카드 주컴퓨터(52)로 전송한다(제104단계). 선불카드 주컴퓨터(52)는 수신된 메시지를 디코딩한 후 데이터베이스(54)에 해당 카드의 제1 고유번호 및 잔액을 조회한다(제106단계).

주컴퓨터(52)는 인증 요청 메시지에 포함된 제1 고유번호를 데이터베이스(54)에서 독출된 것과 비교하여 두 번호가 동일한 것인지 판단한다. 또한, 주컴퓨터(52)는 인증 요청 메시지에 포함된 사용 금액이 데이터베이스(54)에 저장된 잔액보다 작은지 여부를 판단한다. 판단 결과에 따라, 주컴퓨터(52)는 VAN 호스트(40)를 경유하여 CAT(30)에 인증 응답 메시지를 전송한다(제108단계, 제110단계). 만약 인증 요청 메시지에 포함된 제1 고유번호가 데이터베이스(54)에 저장된 것과 동일하고 해당 카드의 잔액이 인증 요청 메시지에 포함된 사용 금액보다 많다면, 인증 응답 메시지에는 사용 승인 정보와 함께 잔액 정보가 포함된다. 만약 인증 요청 메시지에 포함된 고유번호가 데이터베이스(54)에 저장된 것과 동일하지만 데이터베이스에 저장된 잔액이 인증 요청 메시지에 포함된 사용 금액보다 적다면, 인증 응답 메시지에는 잔액 부족을 나타내는 메시지와 함께 잔액 정보가 포함된다. 이처럼 잔액이 모자라는 경우에는, 상품 대금의 일부만을 예컨대 잔액만큼만을 선불카드로 지불하고 부족분은 현금이나 신용카드로 납부하도록 할 수도 있다. 한편, 인증 요청 메시지에 포함된 고유번호가 데이터베이스(54)에 저장된 것과 동일하지 않은 경우에는, 해당 카드가 불법 카드라는 정보와 카드 회수 및 신고 요구만이 인증 응답 메시지에 포함된다.

사용을 승인하는 인증 응답 메시지를 수신한 경우, CAT(30)는 영수증을 발행하고 카드 잔액 안내 메시지를 디스플레이 해준다(제112단계). 영수증 발급이 완료된 후, CAT(30)는 VAN 호스트(40)를 경유하여 거래 결과를 선불카드 주컴퓨터(52)에 전송한다(제114, 제116 단계). 이에 따라, 선불카드 주컴퓨터(52)는 거래 결과를 반영하여 잔액 데이터를 수정하고 거래내역을 추가함으로써 데이터베이스(54)를 갱신하게 된다(제118단계).

한편, 선불카드 주컴퓨터(52)는 정기적으로 각 가맹점별 선불카드 수납내역 및 각 선불카드의 잔액 데이터를 카드발행사 웹서버(70)에 전송한다. 이러한 데이터가 VAN 사업자 및/또는 각 가맹점에 전송될 수도 있다(제120단계). 카드발행사는 정기적 또는 비정기적으로 각 가맹점별 선불카드 결제액을 가맹점 주에게 입금한다(제122단계). 결제액 입금은 선불카드 주컴퓨터 부시스템(50) 운영자, VAN 사업자 또는 기타 카드관리업체를 통해 이루어질 수도 있다. 결제액 입금 방식에 따라 카드발행사와, 선불카드 주컴퓨터 부시스템(50) 운영자 또는 VAN 사업자간의 정산 시기나 비율 등 정산 방식이 달라질 수 있다.

도 9는 전자상거래에 있어서의 선불카드 인증 절차의 일 실시예를 보여준다. 카드 소지자가 전자상거래를 통해 상품을 구매하고자 하는 경우, 카드 소지자는 먼저 본 발명에 의한 선불카드의 사용이 가능한 쇼핑몰(70, 72a 또는 72b)에 접속한다. 이때 쇼핑몰(70, 72a 또는 72b)은 선불카드의 사용 가능 여부를 초기 화면에 표시할 수 있다. 원하는 상품을 쇼핑바구니에 넣음으로써 상품을 주문한 후, 구매자는 '결제'

버튼을 눌러 결제 단계로 진행할 수 있다(제130단계).

결제를 위한 웹페이지 내에는 선택가능한 결제 방법들 중 하나를 선택하기 위한 복수의 버튼들이 표시되는데, 그 중에는 '선불카드로 결제' 버튼이 포함된다. 이때, 만약 여러 종류의 선불카드가 사용가능할 때에는 각 선불카드 종류에 대하여 별도의 버튼이 마련되는 것이 바람직하다. 카드 소지자가 '선불카드로 결제' 버튼을 누르면(제132단계), 쇼핑몰(70, 72a 또는 72b)은 구매자에게 비밀번호 및 제2 고유번호를 입력할 것을 요구하게 된다(제134단계). 구매자가 비밀번호 및 제2 고유번호를 입력하고 '확인' 버튼을 누르게 되면, 비밀번호 및 제2 고유번호는 쇼핑몰(70, 72a 또는 72b)로 전송된다(제136단계).

비밀번호 및 제2 고유번호를 받아들이면, 쇼핑몰(70, 72a 또는 72b)은 비밀번호, 제2 고유번호 및 결제금액을 포함하는 인증 요청 메시지를 선불카드 주컴퓨터 부시스템(50)에 전송한다(제138단계). 주컴퓨터(52)는 인증 요청 메시지에 포함된 비밀번호 및 제2 고유번호를 데이터베이스(54)에 저장된 대응 데이터들과 비교하여 각각이 동일한 것인지를 판단한다(제140단계). 또한, 주컴퓨터(52)는 인증 요청 메시지에 포함된 사용 금액이 데이터베이스(54)에 저장된 잔액보다 작은지 여부를 판단한다. 판단 결과에 따라, 주컴퓨터(52)는 쇼핑몰(70, 72a 또는 72b)에 인증 응답 메시지 및 잔액 데이터를 전송한다(제142단계).

카드 사용을 승인하는 인증 응답 메시지를 수신한 경우, 쇼핑몰(70, 72a 또는 72b)은 결제 처리를 수행한 후 결제 처리가 완료되었음을 표시하는 메시지를 클라이언트 컴퓨터(84)에 전송한다(제144단계). 그 다음, 쇼핑몰(70, 72a 또는 72b)은 거래 결과를 선불카드 주컴퓨터(52)에 전송한다(제146단계). 이에 따라, 선불카드 주컴퓨터(52)는 거래 결과를 반영하여 잔액 데이터를 수정하고 거래내역을 추가함으로써 데이터베이스(54)를 갱신하게 된다(제148단계).

한편, 선불카드 주컴퓨터(52)는 정기적으로, 예컨대 매일 1회씩, 각 쇼핑몰(70, 72a 또는 72b)에서의 선불카드 수납내역 및 각 선불카드의 잔액 데이터를 카드발행사 웹서버(70)에 전송한다(제150단계). 이를 토대로 카드발행사는 정기적 또는 비정기적으로 선불카드 결제액을 각 쇼핑몰 운영자에게 주에게 입금하게 된다(제152단계). 대면거래에 있어서와 마찬가지로, 결제액 입금은 선불카드 주컴퓨터 부시스템 운영자(50) 또는 기타 카드관리업체를 통해 이루어질 수도 있다.

도 10a 및 도 10b는 전자상거래시에 있어서의 선불카드 인증 절차의 다른 실시예를 보여준다. 도 9에 도시된 실시예에 있어서는 쇼핑몰(70, 72a 또는 72b)이 직접 클라이언트 컴퓨터(84)로부터 비밀번호 및 제2 고유번호를 받아들이고 이후 선불카드 주컴퓨터(52)에 전송하여 인증을 받는 반면에, 도 10a 및 도 10b에 도시된 실시예에 있어서는 구매자가 선불카드에 의한 결제를 원할 경우 클라이언트 컴퓨터(84)가 선불카드 주컴퓨터(52)에 접속되게 하여 선불카드 주컴퓨터(52)가 비밀번호 및 제2 고유번호를 받아들이도록 하게 된다.

먼저, 도 9의 실시예에 있어서와 마찬가지로, 카드 소지자는 쇼핑몰(70, 72a 또는 72b)에서 원하는 상품을 선택한 후, '결제' 버튼을 눌러 결제 단계로 진행할 수 있다(제160단계). 이때, '선불카드로 결제' 버튼을 누르면(제162단계), "인증 사이트로 이동합니다"라는 메시지가 브라우저 상에 표시됨과 동시에 추후 다시 쇼핑몰(70, 72a 또는 72b)로 돌아오는데 필요한 쿠키(Cookies) 정보가 쇼핑몰 웹서버에서 브라우저로 다운로드되어 저장된다(제164단계). 그 다음, 자동적으로 브라우저는 선불카드 주컴퓨터(52)에 접속되는데, 이때 선불카드 주컴퓨터(52)에 접속하기 위한 http요구의 URL의 헤더에는 결제금액 정보가 포함된다(제166단계).

선불카드 주컴퓨터(52)가 구매자에게 비밀번호 및 제2 고유번호를 입력할 것을 요구하고(제168단계) 이에 따라 구매자가 비밀번호 및 제2 고유번호를 입력하고 '확인' 버튼을 누르게 되면, 비밀번호 및 제2 고유번호는 선불카드 주컴퓨터(52)로 전송된다(제170단계). 주컴퓨터(52)는 입력된 비밀번호 및 제2 고유번호와 결제금액을 데이터베이스(54)에 저장된 대응 데이터들과 비교하여 각각이 동일한 것인지를 판단한다(제172단계). 또한, 주컴퓨터(52)는 결제대금이 데이터베이스(54)에 저장된 잔액보다 작은지 여부를 판단한다. 판단 결과에 따라, 주컴퓨터(52)는 클라이언트 컴퓨터(84)에 승인 메시지를 포함하는 웹문서를 전송한다(제174단계).

상기 웹문서를 수신한 구매자가 문서 하단에 있는 '쇼핑몰로 되돌아가기' 버튼을 누르면(제176단계), 웹브라우저는 쿠키를 사용하여 쇼핑몰(70, 72a 또는 72b)에 재접속하게 된다(제178단계). 재접속이 이루어지면, 쇼핑몰 웹서버는 결제 처리를 수행한 후 결제 처리가 완료되었음을 표시하는 메시지를 클라이언트 컴퓨터(84)에 전송한다(제180단계). 도 10b에 도시된 제182단계 내지 제186단계는 도 9의 제146단계 내지 제152단계와 동일하므로, 이에 대한 자세한 설명은 생략한다.

한편, 피막 아래에 인쇄되어 있는 제2 고유번호가 노출되어 타인이 불법적으로 사용하는 것을 방지하기 위하여, 본 발명의 선불카드 사용 내지 인증 과정에 있어서는 다양한 방안이 취해질 수 있다. 먼저, 전자상거래를 이용하지 않는 선불카드 구매자들에 대해서는 피막을 벗기지 말도록 홍보 내지 교육하는 것이 필요하다. 카드를 분실하거나 도난당한 경우, 원 구매자 또는 이를 양도받은 정당한 권리자는 인터넷 또는 ARS를 통해서 자신의 카드의 제2 고유번호 또는 비밀번호를 제시한 후 타인의 대면거래 사용을 금지시킬 수 있다. 이러한 경우 정당한 권리자는 인터넷을 통한 전자상거래를 통해 계속 사용할 수 있다. 또한, 카드 표면에 인쇄된 제2 고유번호를 이용하여 타인이 정당한 권리자로 가장하여 이용자번호 및 비밀번호를 부여받는 경우에 대비하여, 초기 비밀번호 등록시에 성명, 주민등록번호 및 전자우편 주소 등을 입력하게 하여 신상을 파악해둘 수도 있다.

또한, 선불카드를 사용하여 쇼핑몰에서 상품을 구매할 때 카드의 제2 고유번호가 해킹되는 것을 방지하고 데이터 전송의 신뢰성을 높이기 위하여, 각 거래시마다 제2 고유번호의 특정 자리수(예컨대, 마지막 네 자리)를 변경하도록 요구할 수도 있다. 또한, 다른 실시예에 있어서는, 카드 표면에 제2 고유번호를 여러 개 인쇄하여 각 거래시마다 이용 특정 번호를 입력하도록 지시할 수도 있다.

이상의 설명은 본 발명의 바람직한 실시예를 예시하는 것으로서, 본 발명은 이에 한정되지 않고 다양하게 변형될 수 있다. 예컨대, 고액 상품권의 경우 각 선불카드에 위에서 기술한 일련번호 및 제1 및 제2 고유번호이외에 별도의 비밀번호를 서면으로 알려주고, 카드 소지자가 카드를 사용함에 있어서 카드 승인

단말기에 부착된 핀패드(PIN Pad)를 통해 상기 비밀번호를 입력하게 할 수도 있다. 이러한 비밀번호는 카드 소지자가 자동응답 부시스템(55)에 잔액을 조회할 때에도 사용될 수 있다. 또한, 인터넷을 통한 전자상거래 시에 해킹을 방지하기 위하여 보안 알고리즘으로 데이터를 보호할 수도 있다.

바람직한 실시예에 있어서는 카드 승인 단말기로 신용카드용 CAT가 사용되지만, 본 발명의 다른 실시예에 있어서는 선불카드 데이터 독출을 위한 다른 종류의 단말기가 사용될 수도 있다. 아울러, 백화점과 같은 대형 유통점 내에서의 대면거래에 있어서는 CAT 대신에 POS 단말기가 사용될 수 있는데, 이러한 경우 POS 단말기에 의해 입력된 제1 고유정보와 결제 금액 데이터는 카드 VAN 호스트(40)를 거치지 않고 직접 선불카드 주컴퓨터에 접속될 수도 있다. 이러한 경우, 카드 승인 단말기 운영자는 카드 VAN 호스트에 대한 접속료를 지불할 필요가 없게 된다.

선불카드 소지자는 인터넷을 통해 선불카드 주컴퓨터(50) 또는 카드발행사 웹서버(70)에 접속한 상태에서 신용카드로 선불카드를 재충전하거나 잔액을 증가시킬 수도 있다. 이러한 변형예는 본 발명이 속하는 기술분야의 당업자가 용이하게 실시할 수 있는 것이므로 구체적인 설명을 생략하기로 한다. 또한, 재충전 기능을 수행하는 시스템은 대면거래와 전자상거래에서 사용 금액이 많은 사용자에 대해서 보상금을 이체해 줄 수도 있다. 이러한 재충전 기능으로 말미암아 본 발명의 선불카드는 전자화폐의 차원까지 확대될 수도 있다.

한편, 도 6에는 신용카드 VAN 호스트(40), 선불카드 주컴퓨터(50) 등이 하나의 컴퓨터인 것으로 표시되어 있지만, 이들 각각이 물리적으로 다수의 컴퓨터로 구성될 수도 있다. 다른 한편으로, 카드 VAN 호스트(40)와 선불카드 주컴퓨터 부시스템(50)은 동일한 운영자에 의해 운영될 수도 있으며, 이러한 경우 이들 두 개의 부시스템이 하나의 물리적 시스템 내에서 구현될 수도 있다. 마찬가지로 선불카드 주컴퓨터 부시스템(50) 및 카드발행사 웹서버(70) 역시 동일한 운영자에 의해 운영될 수도 있으며, 이러한 경우 이들 두 개의 부시스템이 하나의 물리적 시스템 내에서 구현될 수도 있다.

또한 이상의 설명에 있어서는 카드 발행업체가 자신이 판매할 선불카드를 직접 제작하는 것과 같이 설명하였지만, 실제에 있어서는 선불카드 발행업체와 카드 제작업체가 분리되어 있을 수 있다. 이러한 경우 카드 제작업체는 카드 매체를 생산하고 선불카드 발행업체가 제공하는 난수 데이터를 기록하는 단순 임가공 업무만을 수행한다. 따라서, 이와 같이 선불카드 발행업체와 카드 제작업체가 분리되어 있는 경우, 이상의 설명에서 기재된 '카드 발행업체'라는 용어는 카드 제작업체에게 제작을 의뢰하여 제작된 카드를 판매하는 업체를 의미하는 것으로 해석하여야 하며, 제작업체의 행위는 실질적으로 카드 발행업체에 의해 행해지는 것으로 해석해야만 한다.

상술한 바와 같이, 본 발명이 속하는 기술분야의 당업자는 본 발명이 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로서 이해해야만 한다. 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 등가개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

발명의 효과

본 발명에 따르면, 대면거래에 선불카드를 사용함에 있어서 전용 단말기가 반드시 필요한 것은 아니며 기존의 신용카드 승인 단말기를 통해 인증을 받을 수 있다. 따라서, 선불카드가 선불카드 전용 단말기에만 한정적으로 사용되는 것이 아니고, 소규모 슈퍼마켓, 대여점, 음식점, 주유소 등 신용카드 승인 단말기가 설치된 곳이라면 어느 곳이든지 사용이 가능해진다. 이에 따라, 선불카드 가맹점들의 설비비 부담이 감소하며, 구매자의 입장에서도 대면거래에 있어서의 선불카드의 효용이 크게 증대된다.

본 발명에 바람직한 실시예들에 따르면 제1 및 제2 고유번호가 모두 난수발생기에 의해 발생되기 때문에, 어느 한 카드의 고유번호를 알아냈다 해도 그 카드와 일련 번호가 연이어진 다음 카드의 고유번호를 예측하는 것은 거의 불가능하다. 또한 선불카드는 일반적으로 액면가가 그리 높지 않기 때문에, 어느 한 카드가 어떤사람 위조 또는 변조되었다 해도 카드 발행 업체가 입는 피해는 크지 않고 또한 그 피해는 일회성에 그치게 된다.

특히, 선불카드가 일종의 무기명 채권인 점을 고려하여 이러한 피해는 진정한 카드 소유주에게 전가될 수도 있다. 더욱이, 단말기에서 독립적으로 카드 사용을 승인하고 잔액을 기입하게 되는 경우에는 위조된 동일 고유번호의 선불카드를 동시에 여러 곳에서 사용할 때 실시간으로 확인하는 것이 어렵지만, 본 발명에 있어서는 선불카드의 잔액 정보를 중앙집중식으로 관리하고 유지하고 잔액 한도에서만 카드를 사용할 수 있기 때문에, 복수의 위조 카드를 동시에 여러 곳에서 사용하는 것이 불가능하고 위조 및 변조에 따른 피해 가능성은 더욱 줄어들게 된다.

아울러, 본 발명은 두 개의 난수를 하나의 계정 단위로 관리하여 전자상거래 및 대면거래시마다 잔액을 차감하여 실시간으로 사용 이력을 관리하게 된다. 또한, 카드 소지자는 인터넷을 통해서 또는 ARS를 통해서 자신의 카드에 인쇄된 제2 고유번호를 입력하고 전자상거래 및 대면거래를 포함하는 모든 거래 이력을 조회할 수 있다. 이에 따라 하나의 카드를 전자상거래 및 대면거래 모두에 대해 편리하게 사용할 수 있게 된다.

한편, 본 발명의 바람직한 실시예에 있어서는 선불카드의 매체로써 자기 스트립이 증착된 플라스틱 또는 PET 카드가 사용되기 때문에, 카드는 제작 및 관리비용이 다른 매체에 비해 크게 낮다는 장점도 가진다. 또한, 선불카드가 일반적으로 상품권으로서 유통되는 점을 감안할 때, 본 발명에 의한 선불카드는 종이 상품권에 비해 휴대하기가 간편하고 구겨짐이나 물기 또는 습기로부터 안전하다는 장점을 가진다.

(57) 청구의 범위

청구항 1. 대면거래 및 전자상거래 시에 지불 브로커 시스템에 의한 인증 및 잔액 관리를 토대로 대금

지불에 사용될 수 있는 선불카드를 발행하는 방법으로서,

(a) 카드 매체를 마련하는 단계;

(b) 대면거래 시의 인증을 위한 제1 난수와, 전자상거래 시의 인증을 위한 제2 난수를 발생하는 단계; 및

(c) 상기 제1 난수에 관한 정보 및 상기 제2 난수를 상기 카드 매체에 기록하는 단계;

를 포함하는 선불카드 발행 방법.

청구항 2. 제1항에 있어서, 상기 카드 매체는 정보 저장 수단을 포함하고 있으며,

상기 (c)단계는

(c1) 상기 제1 난수 정보를 상기 정보 저장 수단에 저장하는 단계;

를 포함하는 선불카드 발행 방법.

청구항 3. 제1항 또는 제2항에 있어서,

상기 제1 난수 정보는 상기 제1 난수와 동일하며, 따라서 상기 (c)단계에서는 상기 제1 난수 그 자체를 저장하는 선불카드 발행 방법.

청구항 4. 제1항 또는 제2항에 있어서,

상기 (c)단계 수행전에 상기 제1 난수를 암호화하는 단계를 더 포함하며,

상기 (c)단계에서는 암호화된 제1 난수를 저장하는 선불카드 발행 방법.

청구항 5. 제1항 또는 제2항에 있어서, 상기 (c)단계는

(c2) 제2 난수를 상기 카드 매체의 표면에 인쇄하는 단계;

를 더 포함하는 선불카드 발행 방법.

청구항 6. 제3항에 있어서, 상기 (c)단계는

(c3) 상기 제2 난수가 인쇄된 상기 카드 매체 표면 부분에 상기 제2 난수가 노출되는 것을 방지하기 위한 피막을 입히는 단계;

를 더 포함하는 선불카드 발행 방법.

청구항 7. 난수 발생기에 의해 발생되는 제1 및 제2 난수를 토대로 각각 결정되는 제1 및 제2 고유번호를 포함하는 복수의 고유번호들이 기록된 선불카드에 의해 상품 결제 대금을 결제할 수 있도록 하기 위하여, 상기 선불카드를 인증하고 상기 선불카드의 잔액 데이터를 관리하는 방법으로서,

(a) 카드 승인을 위한 단말기와, 상기 제1 및 제2 고유번호와 동일할 것이 요구되는 제1 및 제2 발행 고유번호와 상기 잔액 데이터를 저장하는 호스트를 제공하는 단계;

(b) 구매자가 대면거래를 통해 상기 상품을 구매하고자 하는 경우, 상기 단말기를 통해 상기 제1 고유번호 및 제1 결제대금 데이터를 받아들이고 상기 제1 고유번호 및 상기 제1 결제대금 데이터를 각각 상기 제1 발행 고유번호 및 상기 잔액 데이터와 비교하는 단계;

(c) 상기 (b)단계에서 상기 제1 고유번호 및 상기 제1 발행 고유번호가 서로 동일하고 잔액이 0이 아닌 경우 승인액 만큼의 상기 선불카드의 사용을 승인하되, 상기 잔액이 상기 제1 결제대금보다 많은 때에는 상기 승인액은 상기 제1 결재대금이고 상기 잔액이 상기 제1 결제대금보다 적은 때에는 상기 승인액은 상기 잔액인 단계;

(d) 구매자가 전자상거래를 통해 상기 상품을 구매하고자 하는 경우, 상기 전자상거래가 이루어지는 머천트 서버로부터 상기 제2 고유번호 및 제2 결제대금 데이터를 받아들이고 상기 제2 고유번호 및 상기 제2 결제대금 데이터를 각각 상기 제2 발행 고유번호 및 상기 잔액 데이터와 비교하는 단계;

(e) 상기 (d)단계에서 상기 제2 고유번호 및 상기 제2 발행 고유번호가 서로 동일하고 잔액이 0이 아닌 경우 승인액 만큼의 상기 선불카드의 사용을 승인하되, 상기 잔액이 상기 제2 결제대금보다 많은 때에는 상기 승인액은 상기 제2 결재대금이고 상기 잔액이 상기 제2 결제대금보다 적은 때에는 상기 승인액은 상기 잔액인 단계; 및

(f) 상기 선불카드의 사용을 승인한 경우, 상기 잔액에서 상기 승인액을 차감하여 차감된 잔액을 수정된 잔액으로서 다시 저장하는 단계;를 포함하는 선불카드 인증 및 잔액 데이터 관리 방법.

청구항 8. 제7항에 있어서, 상기 선불카드는 정보 저장을 위한 정보 저장 수단을 구비하고 있는 선불카드 인증 및 잔액 데이터 관리 방법.

청구항 9. 제8항에 있어서, 상기 선불카드는 자기 스트립을 구비하는 자기 스트립 카드 형태로 되어 있는 선불카드 인증 및 잔액 데이터 관리 방법.

청구항 10. 제9항에 있어서, 상기 단말기는 상기 선불카드는 물론 일반적인 신용카드를 판독할 수 있는 신용카드 승인 단말기 및 POS 단말기 중에서 선택되는 어느 하나인 선불카드 인증 및 잔액 데이터 관리 방법.

청구항 11. 제6항에 있어서, 상기 제1 고유번호는 상기 선불카드의 정보 저장 수단에 저장되어 있고, 상기 제2 고유번호는 상기 선불카드의 표면에 인쇄되어 있는 선불카드 인증 및 잔액 데이터 관리 방법.

청구항 12. 제7항 내지 제11항 중 어느 한 항에 있어서, 상기 제2 고유번호는 상기 제2 난수와 동일한

데이터인 선불카드 인증 및 잔액 데이터 관리 방법.

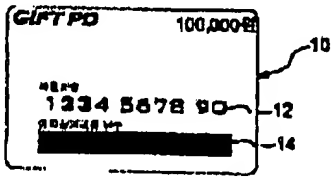
청구항 13. 제7항 내지 제11항 중 어느 한 항에 있어서,

(s) 상기 선불카드의 소지자의 요구에 응답하여 상기 잔액을 안내하는 단계;

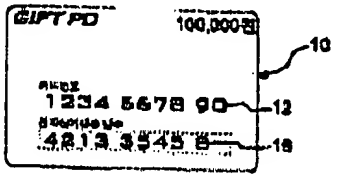
를 더 포함하는 선불카드 인증 및 잔액 데이터 관리 방법.

도면

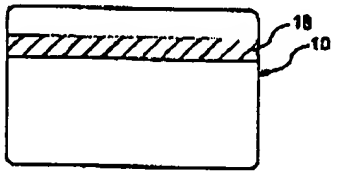
도면1



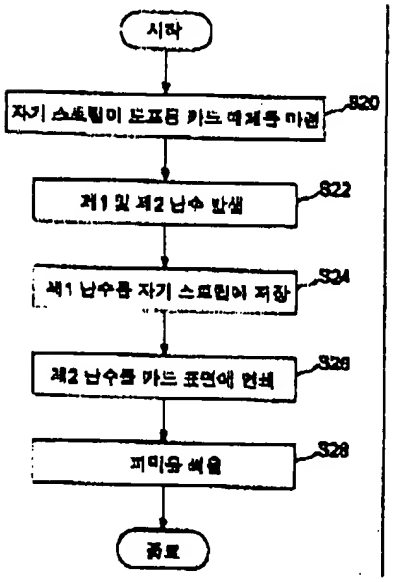
도면2



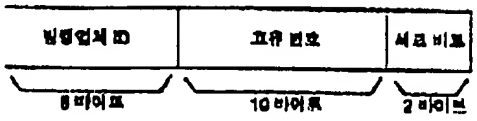
도면3



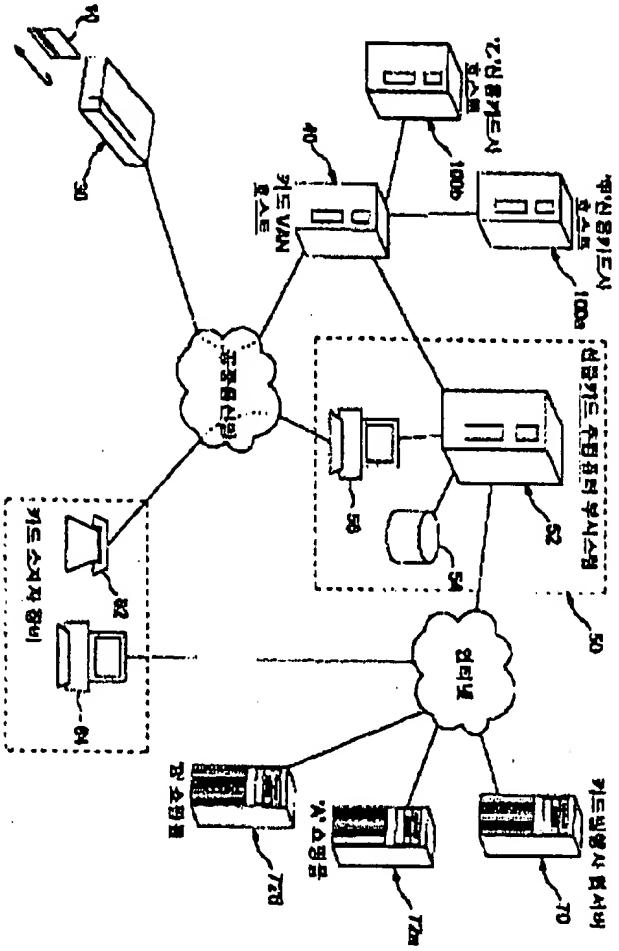
도면4



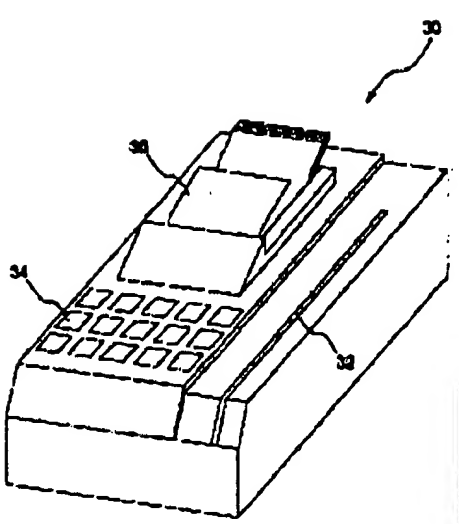
도면5


업종업태 ID
고유 번호
체크 비트
8 바이트
10 바이트
2 바이트

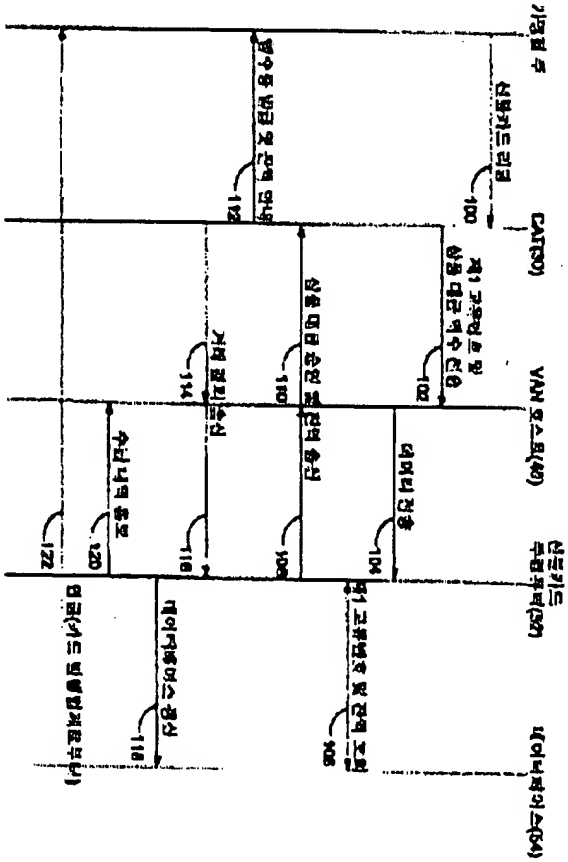
도면6


30
40
카드 VAN 호스트
1000
1002
50
52
54
56
58
60
62
64
70
72a
72b
72c
인터넷

도면7

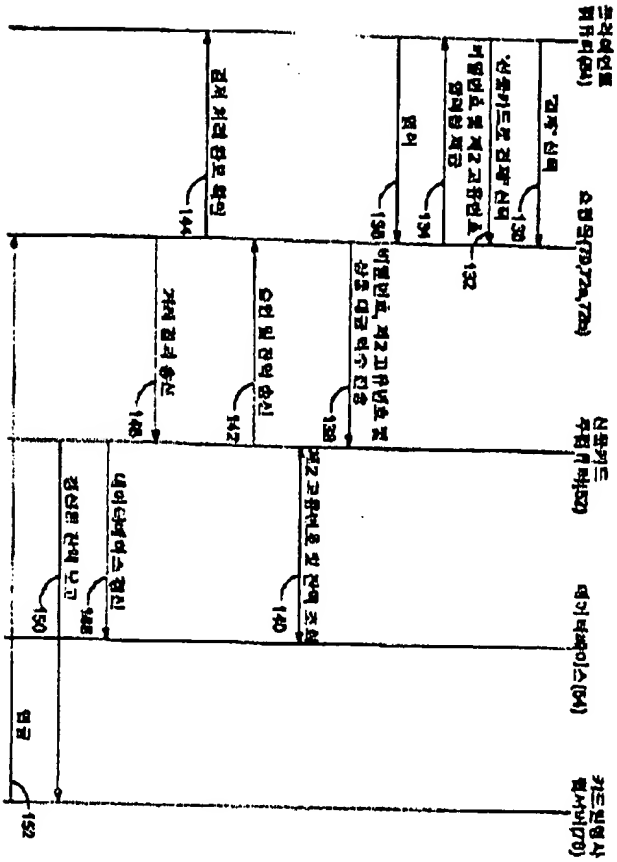

38
36
34
32

도면8

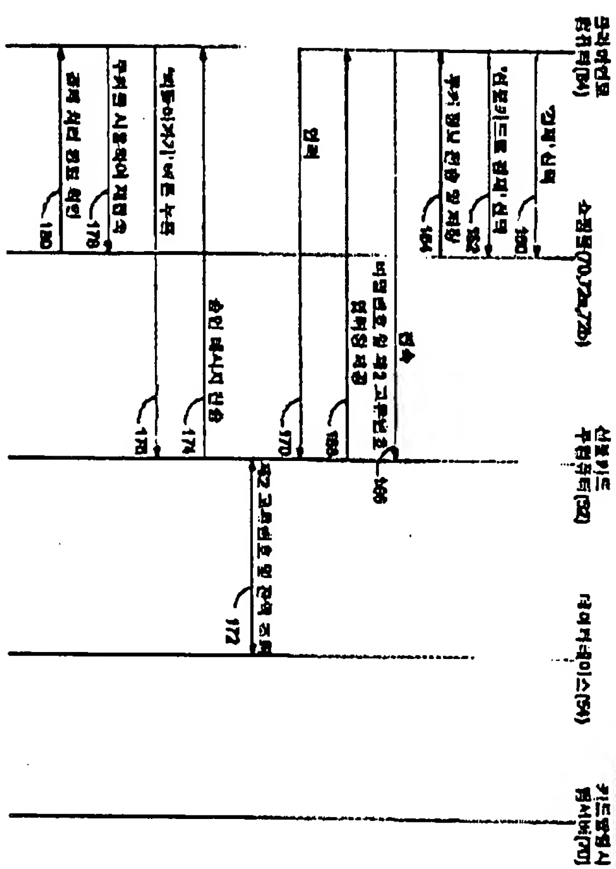

사용자 I/F
CATOS
VAN 소프트웨어
실시간 운용 소프트웨어
하드웨어 (VAN)
100
102
104
106
108
110
112
114
116
118
120
122

2000-0049518

도면



도면 10a



特2000-0049518

도면16